EU-RAIL SYSTEM PILLAR

Securing External Communication Interfaces

Version: 1.1.1

Securing External Communication Interfaces

Document data

Created by	System Pillar Cybersecurity Domain
Classification	Public
Status	Released
Version	1.1.1
Date	28-OCT-2026

Copyright

© Europe's Rail Joint Undertaking, 2026

This document is drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

EU Rail authorises you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following: EU Rail trade mark, title of the document, year of publication, version of document.

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models in this document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trade marks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

Document History

Version	Date	Description	Status
1.1.1	28-OCT-2026	Release for ERA Technical Documents	released
1.1	23-MAR-2026	Error correction and additional guidance for version 1.0	released
1.0	20-FEB-2025	Initial public release	released

Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address: cybersecurity.review@ertms.be

1 Table of Contents

1 Table of Contents 4
2 Preamble 5
2.1 Scope, Purpose and Intended Audience 5
2.2 Document Usage 5
2.3 References 5
3 Identification, Authentication and Authorization 6
4 Communication Integrity and Confidentiality 6
5 Access Logging 7
6 DoS Resilience and Minimising Negative Impact 7

2 Preamble

2.1 Scope, Purpose and Intended Audience

, SP-SEC-CommExt-2.1-1 - This document contains requirements for additional communication interfaces using other communication protocols which are not defined in this specification. These requirements are required to achieve compliance to EU CRA and IEC 62443-4-2.
Examples of other communication interfaces: SSH, FTPS,... **[**SPPRAMSS-18606 **]**

, SP-SEC-CommExt-2.1-2 - In general, all maintenance and diagnostic activities should be conducted using existing interfaces (e.g. SDI, SMI,...).
Direct access to the operating system is not advisable and should be avoided. **[**SPPRAMSS-18604 **]**

, SP-SEC-CommExt-2.1-3 - As per EU-CRA and IEC 62443-4-2, the attack surface of a device is required to be limited. Therefore, additional communication interfaces should only be added, if there are essential for the operation and can not be avoided. See corresponding SP-SEC-CompSpec Ch 5.3.6 - Hardening for corresponding requirements. **[**SPPRAMSS-18605 **]**

, SP-SEC-CommExt-2.1-4 - If specific other communication protocols are used extensively, this specification can be extended to define a security profile for the specific protocol to allow interoperability between communications partners. **[**SPPRAMSS-18603 **]**

2.2 Document Usage

, SP-SEC-CommExt-2.2-1 - This specification uses identifiers starting with "SP-SEC-CommExt". **[**SPPRAMSS-18608 **]**

, SP-SEC-CommExt-2.2-2 - Icon types used in this document are defined in SP-SEC-Tax. **[**SPPRAMSS-18612 **]**

, SP-SEC-CommExt-2.2-3 - For a definition of the words "shall", "should" and "may" used in this specification, refer to SP-SEC-CommExt-2.3-2 - [ISO/IEC Directives, Part 2] . **[**SPPRAMSS-18613 **]**

2.3 References

, SP-SEC-CommExt-2.3-1 - This chapter contains all references of this document. For a complete list including external references see [SP-SEC-Tax] Chapter 3. **[**SPPRAMSS-14017 **]**

[ISO/IEC Directives, Part 2]
Principles and rules for the structure and drafting of ISO and IEC documents

[RFC 5280]
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

3 Identification, Authentication and Authorization

, SP-SEC-CommExt-3-1 - Each software process realising an additional communication interface shall be capable of identifying itself and authenticating to any other communication partner using a unique X.509 v3 certificate as defined in SP-SEC-CommExt-2.3-3 - [RFC 5280] or an equally secure method.
Note1: recommendation is to use a unique X.509 certificate
Note2: there should be a way to identify a software process (web server, safety communication, diagnostics server,...), not per software process instance of the same software process. **[**SPPRAMSS-2967 **]**

, SP-SEC-CommExt-3-2 - Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity.
Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable.
[SPPRAMSS-3999 **]**

, SP-SEC-CommExt-3-3 - Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization.

Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication.
Note2: in case of non-availability of the IAM, local accounts can be used **[**SPPRAMSS-2310 **]**

, SP-SEC-CommExt-3-4 - Each software process realizing an additional communication interface shall enforce access based on retrieved permissions.
Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component. **[**SPPRAMSS-2311 **]**

4 Communication Integrity and Confidentiality

, SP-SEC-CommExt-4-1 - Each software process realizing an additional communication interface shall protect the integrity of data in transit.
Note: this should, if applicable, be realized preferable using TLS with an integrity cipher. In any case, a cryptographic method for integrity protection is required
[SPPRAMSS-2478 **]**

, SP-SEC-CommExt-4-2 - If data in transit is considered confidential, a software process realizing an additional communication interface shall provide the capability to protect the confidentiality of data in transit.
Note: this should, if applicable, be realized preferable using TLS with an encryption cipher.
Examples of confidential data in transit are encryption keys, legally protected personal data, user credentials, person/user related data, financial information, security related logs and/or diagnosis data. **[**SPPRAMSS-6887 **]**

5 Access Logging

, SP-SEC-CommExt-5-1 - Security logging for communication interface accesses is required by EU CRA and IEC 62443-4-2. Corresponding requirements can be found in SP-SEC-CompSpec-5.7 - Logging and Diagnostic **[**SPPRAMSS-13119**]**

6 DoS Resilience and Minimising Negative Impact

, SP-SEC-CommExt-6-1 - DoS resilience for communication interfaces is required by EU CRA and IEC 62443-4-2.
Corresponding requirements can be found in SP-SEC-CompSpec-5.4.4 Denial of service resilience **[**SPPRAMSS-13117**]**

, SP-SEC-CommExt-6-2 - Minimising negative impact to network and to connected devices is required by EU CRA.
Corresponding requirements can be found in SP-SEC-CompSpec-5.4.2 Host-based firewall **[**SPPRAMSS-13118**]**